CLAIMS:

1. An apparatus for performing a SubByte function of the Rijndael Block Cipher, comprising:

an S-box constructed by composing a first and second transformation, wherein the first transformation is a look-up table (300), and the second transformation is an affine-all transformation that performs both an affine and inverse affine transformation.

2. The apparatus as claimed in claim 1, wherein:

the look-up table (300) is the multiplicative inverse in the finite field GF(2^8) having {00} mapped to itself; and

the affine-all transformation is implemented using a combinational logic circuit (400).

3. The apparatus as claimed in claim 2, wherein:

the look-up table (300) is implemented by a read-only memory (ROM); and

the combinational logic circuit (400) implements the equations

$$
\begin{aligned}
b'_0&=[(b_0 \cong p_0)\rho(b_1 \cong p_1)\rho(b_2 \cong p_2)\rho(b_3 \cong p_3)\rho(b_4 \cong p_4)\rho(b_5 \cong p_5)\rho(b_6 \cong p_6)\rho(b_7 \cong p_7)]\rho v_0\\
b'_1&=[(b_0 \cong p_7)\rho(b_1 \cong p_0)\rho(b_2 \cong p_1)\rho(b_3 \cong p_2)\rho(b_4 \cong p_3)\rho(b_5 \cong p_4)\rho(b_6 \cong p_5)\rho(b_7 \cong p_6)]\rho v_1\\
b'_2&=[(b_0 \cong p_6)\rho(b_1 \cong p_7)\rho(b_2 \cong p_0)\rho(b_3 \cong p_1)\rho(b_4 \cong p_2)\rho(b_5 \cong p_3)\rho(b_6 \cong p_4)\rho(b_7 \cong p_5)]\rho v_2\\
b'_3&=[(b_0 \cong p_5)\rho(b_1 \cong p_6)\rho(b_2 \cong p_7)\rho(b_3 \cong p_0)\rho(b_4 \cong p_1)\rho(b_5 \cong p_2)\rho(b_6 \cong p_3)\rho(b_7 \cong p_4)]\rho v_3\\
b'_4&=[(b_0 \cong p_4)\rho(b_1 \cong p_5)\rho(b_2 \cong p_6)\rho(b_3 \cong p_7)\rho(b_4 \cong p_0)\rho(b_5 \cong p_1)\rho(b_6 \cong p_2)\rho(b_7 \cong p_3)]\rho v_4\\
b'_5&=[(b_0 \cong p_3)\rho(b_1 \cong p_4)\rho(b_2 \cong p_5)\rho(b_3 \cong p_6)\rho(b_4 \cong p_7)\rho(b_5 \cong p_0)\rho(b_6 \cong p_1)\rho(b_7 \cong p_2)]\rho v_5\\
b'_6&=[(b_0 \cong p_2)\rho(b_1 \cong p_3)\rho(b_2 \cong p_4)\rho(b_3 \cong p_5)\rho(b_4 \cong p_6)\rho(b_5 \cong p_7)\rho(b_6 \cong p_0)\rho(b_7 \cong p_1)]\rho v_6\\
b'_7&=[(b_0 \cong p_1)\rho(b_1 \cong p_2)\rho(b_2 \cong p_3)\rho(b_3 \cong p_4)\rho(b_4 \cong p_5)\rho(b_5 \cong p_6)\rho(b_6 \cong p_7)\rho(b_7 \cong p_0)]\rho v_7
\end{aligned}
$$

having $p = p_0p_1p_2p_3p_4p_5p_6p_7$ as a load pattern consisting of {10001111} for the affine transformation and {00100101} for the inverse affine transformation and having v as a load vector = $v_0v_1v_2v_3v_4v_5v_6v_7$ consisting of {11000110} for the affine transformation and {10100000} for the inverse affine transformation.

4. An apparatus for encrypting and decrypting data, comprising:

a data processing module arranged to perform a byte substitution, wherein at least part of said data processing module comprises:

a look-up table (300),

a storage device for storing the look-up table, and

a circuit (400) having shared logic that performs a single transform that accomplishes either an affine and an inverse affine transformation.

5. The apparatus as claimed in claim 4 wherein said look-up table (300) is a multiplicative inverse of the finite field GF(2^8).

6. The apparatus as claimed in claim 5, wherein said look-up table (300) is implemented by means of a read only memory (ROM).

7. The apparatus as claimed in claim 4, wherein said look-up table (300) is implemented by means of a read only memory (ROM).

8. The apparatus as claimed in claim 4, wherein the apparatus comprises a plurality of instances of a data processing module arranged in a data processing pipeline.

9. The apparatus as claimed in claim 4, wherein the apparatus is arranged to perform encryption or decryption in accordance with the Rijndael Block Cipher, and wherein the data processing module is arranged to implement a Rijndael round.

10. An apparatus as claimed in claim 9, wherein the data processing module is arranged to implement the SubByte transformation of the Rijndael round using the look-up table composed with the affine transformation for encryption and the inverse affine transformation for decryption.

11. The apparatus as claimed in claim 10, wherein said look-up table (300) is implemented by means of a read only memory (ROM).

12. A apparatus for performing a SubByte function of a round of the Rijndael Block Cipher, comprising an S-box constructed by composing,

means for obtaining the multiplicative inverse in the finite field GF(2^8), and means for performing an affine-all transformation consisting of an affine and inverse affine transformation as a single affine transformation.

13. The apparatus as claimed in claim 12, wherein said means for obtaining the multiplicative inverse is a look-up table (300), and said means for performing the affine-all transformation is a combinational logic circuit (400).

14. A method for performing a SubByte function of a Rijndael round of the Rijndael Block Cipher, comprising the steps of:

creating a look-up table (300) for the multiplicative inverse in the finite field GF(2^8);

providing an affine-all transformation consisting of an affine and inverse affine transformation in a single affine transformation;

composing an S-box constructed of the look-up table (300) and the affine-all transformation; and

performing a non-linear byte substitution using the composed S-box.

15. The method of claim 14, wherein the providing step further comprises the step of providing a shared logic circuit (400) that performs the single affine transformation.

16. The method of claim 14, further comprising the step of storing the look-up table (300) in a read-only memory (ROM).

17. The method of claim 16, wherein the providing step further comprises the step of implementing a shared logic circuit (400) that performs the single affine transformation.

18. The method of claim 14, wherein:

the look-up table (300) is the multiplicative inverse in the finite field GF(2^8) having {00} mapped to itself; and

the providing step further comprises the step of implementing a combinational logic circuit (400) that performs the single affine transformation (400).